particular, the tracing method is performed by first applying a "burst load" (*i.e.*, a brief but heavy load of transmitted packets) to various elements (*i.e.*, network links or routers) in the network in turn, and then measuring the change in the rate with which the stream of packets arrives at the target. If the rate is substantially altered *in response to* the application of the given burst load, then it may be deduced that the given element is likely to be somewhere on the path from the source (*e.g.*, the source host of the DoS attack) to the target. If, on the other hand, little or no impact on the rate is observed, then it may be deduced that the given element is unlikely to be along the path traveled by the (attacking) stream of packets. In the latter case, the given element and any networks "behind" it may advantageously be removed from consideration in the attempt to identify the source of the attack. (*See, e.g.*, instant specification, p. 6, lines 1-4 and lines 17-24.)

Specifically, each of the claims of the instant application recites a method or apparatus "*for tracing* a sequence of packets *to a potential source* thereof" comprising steps or means for:

(i) "*applying a burst load* to each of one or more selected network elements;"

(ii) "*measuring changes* in [a] received packet rate *in response to said application of said burst load* to each of said selected network elements;" and

(iii) "*determining said potential source* of said sequence of packets *based on said measured changes* in said received packet rate."

(*See, e.g.*, independent claims 1 and 16. Emphases added.)

In the outstanding Office Action, instant independent claims 1 and 16 stand rejected based, *inter alia*, on the Examiner's allegations that

(a) *Gupta* "discloses a method/apparatus for tracing a sequence of packets to a potential source thereof;"

(b) *Gupta* discloses the step of "[f]or each selected network element, measuring a change in said received packet rate in response to said application of said burst load to said selected network element;"

(c) *Gupta* discloses the step of "[d]etermining said potential source of said sequence of packets based on said measured changes in said received packet rate;" and

(d) *Munger* "teaches applying a burst load to each of one or more selected network elements in said communications network."

Applicant respectfully submits that each of allegations (a) through (d) is erroneous, as

discussed in detail below. As such, the combination of these two references fails to teach or disclose the invention as claimed in the instant independent claims.

First, the Examiner has alleged that (a) *Gupta* "discloses a method/apparatus for tracing a sequence of packets to a potential source thereof." However, nowhere in *Gupta* is a method of "tracing a sequence of packets to a potential source" disclosed or even suggested. Rather, *Gupta* discloses a system which "efficiently distributes processing-intensive loads among a plurality of intermediate stations in a computer internetwork." (*See Gupta* abstract.) More specifically, in the only portion of *Gupta* explicitly cited by the Examiner (*i.e.*, col. 7, line 66 through col. 8, line 4), a technique of "spot-checking" a fraction of packets passing through a given one of these "intermediate stations" to search for unauthorized packets is being described. (*See, e.g., Gupta*, col. 7, lines 19-48.) Neither in this portion of *Gupta* nor any other is "a method/apparatus for tracing a sequence of packets to a potential source thereof" disclosed or even suggested.

Second, the Examiner has alleged that (b) *Gupta* discloses the step of "[f]or each selected network element, measuring a change in said received packet rate in response to said application of said burst load to said selected network element." Again, nowhere in *Gupta* is a change in a received packet rate *in response to the application of a burst load* disclosed or suggested. In fact, the Examiner has admitted that *Gupta* "does not teach applying a burst load to each of one or more selected network elements in said communications network." (*See* Office Action, p. 3.) Moreover, *Gupta* does not teach applying a burst load at all, and, as such, cannot possibly disclose "measuring a change in said received packet rate *in response to said application of said burst load.*" Rather, all that is described by *Gupta* is that if "the switch . . . does detect a change in the traffic pattern, e.g., a significant increase in packet transfer rate from a particular source . . . [then it] may be an indication that a sender is attempting to attack the network by inserting a plurality of unauthorized packets into a stream." (*See Gupta*, col. 7, line 65 through col. 8, line 4.) In other words, *Gupta* discloses only the *passive* detection of a change in the traffic pattern resulting from a possible attack – not a change in packet rate *in response to the application of a burst load*, as is required by the instant claims.

Third, the Examiner has alleged that (c) *Gupta* discloses the step of "[d]etermining said potential source of said sequence of packets based on said measured changes in said received packet rate." However, nowhere does *Gupta* disclose "determining [a] potential source of [a] sequence of packets" at all. Specifically, in the portion of *Gupta* cited by the Examiner, the described response

to the detection of "a change in the traffic pattern" is to "increase the fraction of packets that are inspected." (*See Gupta*, col. 8, lines 4-6.) The reason for such a response is that the system of *Gupta* includes techniques "directed to efficiently detecting and filtering unauthorized traffic," and not techniques directed to tracing packets to a potential source (as in the instant invention). (*See, e.g., Gupta* abstract.)

And fourth, the Examiner has alleged that *Munger* "teaches applying a burst load to each of one or more selected network elements in said communications network," specifically citing col. 10, lines 6-21 thereof. However, Applicants respectfully submit that this portion of *Munger* does *not* describe applying burst loads at all. Rather, it merely describes combining multiple packets into a single "interleave window" (*i.e.*, a single IP packet containing combined payload data from what had been a plural number of packets), and then adding "decoy" or "dummy" data to such a packet stream in order to *level the load* on the system. (*See, e.g., Munger* col. 10, lines 6-16.) As further explained by *Munger*, "it may be desirable . . . to generate more decoy data during low traffic periods so that communication bursts at one point in the Internet cannot be tied to communication bursts at another point to reveal the communicating endpoints." (*See, e.g., Munger* col. 10, lines 16-21.) In other words, *Munger* merely teaches *leveling* the communication load over time by adding dummy or decoy data, so that the presence of high communication levels (*i.e.*, communication bursts) which may *naturally* occur at various points in time cannot be easily characterized (*i.e.*, so that the "communicating endpoints" cannot be identified). As clearly defined in the instant specification, however, a "burst load" is a brief but heavy load of transmitted packets, which is applied in accordance with the principles of the present invention in order to determine whether a given received packet rate is substantially changed as a result thereof. (*See, e.g.*, the instant specification, p. 6, lines 1-2 and lines 14-22.) Thus, if anything, *Munger* teaches away from *applying a burst load* to network elements, since a burst load necessarily ensures the existence of a *high* load (rather than a level load).

For at least the above reasons, Applicants respectfully submit that independent claims 1 and 16 are patentable over the cited references. And since each of the remaining dependent claims (*i.e.*, claims 2-15 and 17-30) depend from one of independent claims 1 and 16, these dependent claims are patentable over the cited references for at least the same reasons.

Specifically, therefore, Applicants submit that all of the instant claims are patentable over the cited references and respectfully submit that the instant application is in condition for allowance. Reconsideration of this application is respectfully requested in light of this submission. The Examiner is invited to telephone Applicant's attorney, Kenneth M. Brown, at (908) 582 – 5998, should there be any questions or issues for discussion in the reconsideration of the pending application.

Respectfully,

Hal Joseph Burch
William R Cheswick

By _____
Kenneth M. Brown, Attorney
Reg. No. 37590
908 – 582 – 5998

Lucent Technologies Inc.

Date: 12/7/05